UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/782,593	02/12/2001	Marc VanHeyningen	05313.00001	9483

7590 07/03/2006

Banner & Witcoff, Ltd.
1001 G Street, N.W.
Washington, DC 20001-4597

EXAMINER	
SON, LINH L D	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 07/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/782,593	MARC VANHEYNINGEN	
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3 and 5-67* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3, and 5-67* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *01/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is responding to the Amendment received on 03/21/06.

2. Claims 1-3, and 5-48 are pending. Claims 49-67 are newly added claims.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-3, 5-8, 10, and 12-20, 22-28, 30-36, 38-43, and 45-48 are rejected under 35 U.S.C. 102(e) as being anticipated by Djakovic, US Patent No 6351539.

5. As per claims 1 and 43:

Djakovic teaches "A method of transmitting data securely over a computer network, comprising the steps of:

(1) establishing a communication path between a first computer and a second computer" in (Col 7:20-30);

"(2) encrypting and transmitting data records between the first computer and the second computer using a reliable communication protocol, wherein each data record incorporates a nonce (RNG) and encrypted text that has been a encrypted using the nonce without reference to a previously transmitted data record" in (Col 4:1-25, and Col 5:50) (*a nonce is a random number. Djakovic teaches that random number generator is a true random sequence generators (Col 5 lines 35-44), which have the property that the generator's equences cannot be reproduced, even with the same input. Therefore, the random number here used to encrypt the data record can not or will not have any reference to a previously transmitted data*); and

"(3) in the second computer, receiving and decrypting the data records transmitted in step (2) by, for each of the received data records, decrypting the incorporated encrypted text ~~by~~ using the incorporated nonce (SR) in combination with a previously shared encryption key (K3) ~~to decrypt each of the data records~~ without reference to a previously received data record" in (Col 4:25-55).

6. As per claims 2, 17, 24, and 31:

Djakovic teaches "The method of claims 1, 16, 23, and 30, further comprising the step of, prior to step (1), establishing a reliable communication path between the first computer and the second computer and exchanging security credentials over the reliable communication path" in (Col 7 lines 32-45).

7. As per claims 3, 25, and 32:

Djakovic teaches "The method of claim 2, wherein the step of exchanging security credentials comprises the step of exchanging an encryption key that is used to encrypt the data records in step (2)" in (Col 7:20-30).

8. As per claims 5, 12, 26, 33, 39, and 45:

Djakovic teaches "The method of claims 1, 10, 23, 30, 38, and 43, [4], wherein the nonce comprises a random number" in (Col 4 lines 5-7).

9. As per claims 6 and 34:

Djakovic teaches "The method of claims 1 and 30 [4], further comprising the step of, in the second computer, verifying for each received data record that the incorporated nonce (*a nonce is a random number. Djakovic teaches that random number generator is a true random sequence generators (Col 5 lines 35-44), which have the property that the generator's equences cannot be reproduced, even with the same input.)* that the nonce has not previously been- received in a previously transmitted data record" in (Col 4 lines 1-25).

10. As per claims 7, 22, 27, and 35:

Djakovic teaches "The method of claims 1, 16, 23, and 30, wherein step (2) comprises the step of embedding an indicator in each of the encrypted data records

incorporate encrypted text that has been ~~are~~ indicating that the encrypted data records are encrypted according to an encryption scheme that encrypts ~~records~~ text without regard to any previously transmitted data records, and wherein step (3) comprises the step of determining whether the indicator is present in each received record and, in response to determining that the indicator is not present, processing each such record differently than if the indicator is set" in (Col 4 lines 1-25, Col 7 lines 32-45).

11. As per claims 8, 13-15, 18, 40, 42, 46, and 48:

The system of claims 17, 10, 14, 17, 38, 41, 43, and 47, wherein the unreliable communication protocol comprises the User Datagram Protocol" in (Col 6 lines 50), and "wherein the reliable communication protocol comprises the Transmission Control Protocol" in (Col 6 lines 50).

12. As per claims 10, 16, 23, 30, and 38:

Djakovic teaches "A method of securely transmitting a plurality of data records to a remote computer using an unreliable communication protocol, comprising: (1) establishing a reliable connection with the remote computer" in (Col 7:20-30);

"(2) exchanging encryption credentials with the remote computer over the reliable connection" in (Col 7:20-30);

"(3) generating a nonce(*a nonce is a random number. Djakovic teaches that random number generator is a true random sequence generators (Col 5 lines 35-44),*

which have the property that the generator's equences cannot be reproduced, even with the same input.) for each of a plurality of data records, wherein each nonce comprises an initialization vector" in (Col 4:1-25, and Col 5:50);

"(4) for each of the plurality of data records, encrypting the data record by

using the corresponding nonce to encrypt text, ~~each of the plurality of data records~~ and

appending the encrypted text and the corresponding nonce to ~~each of~~ the ~~plurality of~~ data record ~~records~~" in (Col 4:1-25, and Col 5:50);

"(5) transmitting the plurality of data records ~~encrypted in step (4)~~ to the remote computer using an unreliable communication protocol (Col 5:50), such that the remote computer can decrypt the text each of the plurality of ~~encrypted~~ data records using the ~~a~~ corresponding nonce extracted from each ~~encrypted~~ data record (SR) and a previously shared encryption key" in (Col 4:25-55).

13. As per claims 14, 41, and 47:

Djakovic teaches "The method of claims 10, 38 and 43, wherein step (6) is performed using an-encryption key previously shared using a reliable communication protocol" in (Col 7:20-30).

14. As per claim 19:

Djakovic teaches "The system of claim 16, wherein the communication protocol client function and the communication protocol server function are compatible with the SOCKS communication protocol" in (Col 6 lines 35-60).

15. As per claim 20,

Djakovic teaches "The system of claim 16, wherein the communication protocol client function and the communication protocol server function are compatible with the SSL/TLS communication protocol" in (Col 6 lines 35-60).

16. As per claims 28 and 36:

Djakovic teaches "The method of claims 23 and 30, wherein establishing the communication path with the remote computer is performed using the Transmission Control Protocol" in (Col 6 lines 3-10), and "encrypting the data records is performed using the User Datagram Protocol" in (Col 6 lines 3-10).

Claim Rejections - 35 USC § 103

17. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

18. Claims 9, 11, 21, 29, 37, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Djakovic in view Lee et al, US Publication No. 2002/0101848A1, hereinafter "Lee".

19. As per claims 9, 21, 29, and 37:

Djakovic does not specifically teaches "The system of claims 1,16, 23, and 30, wherein the step (2) is performed by a proxy server that encrypts data records received from another server. Djakovic only teaches that the secure communication is provided for two computers (Col 7 lines 20-30).

Nevertheless, Lee discloses a "Systems and Methods for On-location, wireless access of web content" invention, which includes an encoder/decoder at the gateway or proxy server (Figure 7B), which process the packet according to the preset rules (Para 0067-71).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Djakovic's invention to include the implementation of the proxy server in the system for a specific application.

20. As per claims 11 and 44:

Djakovic teach "The method of claims 10 and 43, wherein step (6) comprises the step of checking to determine whether each data record received from the client computer is formatted according to a secure unreliable transmission format" in (Col 4:1-25, and Col 5:50).

However, Djakovic does not teach the determination if a particular record is not formatted according to a secure unreliable transmission format, bypassing the decryption using the corresponding nonce. Djakovic does encrypt/decrypt all data regardless of transmission path or port using the corresponding nonce.

Nevertheless, Lee discloses a "Systems and Methods for On-location, wireless access of web content" invention, which includes an encoder/decoder at the gateway or proxy server (Figure 7B), which process the packet according to the preset rules (Para 0067-71). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify the invention to include the rule-based encoder/decoder to process the incoming data accordingly and also can reduce the unnecessary computation process.

21. Claims 49-67 are rejected under 35 U.S.C. 103(a) as being unpatentable over Djakovic in view of Bellare et al, US/Patent No. 5673319, hereinfter "Bellare".

22. As per claims 49, 51, 52, 54:

Djakovic does not teach "The method of claims 23, 50, 30, 53, wherein encrypting the data records using the nonce includes, for each data record:

Employing the incorporated nonce to create a message authentication code corresponding to the incorporated encrypted text; and appending the message authentication code to the data record".

Nevertheless, Bellare discloses the Block Cipher Mode of Operation For Secure, Length-Preserving Encryption" invention, which includes a method of generating a CBC message authentication code (MAC), and concatenate the CBC-MAC with ciphered block (Col 5 lines 5-20, Col 6 lines 50-56).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Djakovi's invention to incorporate Bellare's CBC-MAC teaching to further authenticate each cipher block.

23. As per claims 50, 53, 60, and 67:

Djakovic does not teach "The method of claim 23, wherein encrypting the data records using the nonce includes, for each data record, producing the encrypted text by employing the incorporated nonce as an initialization vector to encrypt plaintext.

Nevertheless, Bellare discloses the Block Cipher Mode of Operation For Secure, Length-Preserving Encryption" invention, which includes a method of incorporating a (CBC-MAC) as the initialization vector (Col 5 lines 5-20, Col 6 lines 50-56).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Djakovi's invention to incorporate Bellare's CBC-MAC teaching to further authenticate each cipher block.

24. As per claim 55:

Djakovic teaches "A method of securely transmitting a plurality of data records to a remote computer using an unreliable communication protocol, comprising:

(1) establishing a reliable connection with the remote computer" in (Col 7:20-30);

(2) exchanging encryption credentials with the remote computer over the reliable connection" in (Col 7:20-30);

(3)generating a nonce for each of a plurality of data records" in (Col 4:1-25, and Col 5:50);

(4) for each of the plurality of data records, encrypting the data record by encrypting text, using the nonce to generate a message authentication code corresponding to the encrypted text, and

appending the encrypted text, the corresponding nonce (*a nonce is a random number. Djakovic teaches that random number generator is a true random sequence generators (Col 5 lines 35-44), which have the property that the generator's equences cannot be reproduced, even with the same input.)* and the message authentication code to the data record" in (Col 4:1-25, and Col 5:50); and

(5) transmitting the plurality of data records to the remote computer using an unreliable communication protocol, such that the remote computer can decrypt the text in each of the plurality of data records using the corresponding nonce extracted from each data record and a previously shared encryption key" in (Col 4:25-55).

However, Djakovic does not teach of "using the nonce to generate a message authentication code corresponding to the encrypted text".

Nevertheless, Bellare discloses the Block Cipher Mode of Operation For Secure, Length-Preserving Encryption" invention, which includes a method of generating a CBC message authentication code (MAC), and concatenate the CBC-MAC with ciphered block (Col 5 lines 5-20, Col 6 lines 50-56).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Djakovi's invention to incorporate Bellare's CBC-MAC teaching to further authenticate each cipher block.

25. As per claims 56, 63, and 67:

Djakovic teaches "The method of claim 55, wherein step (3) comprises generating a random number as each nonce" in (Col 4:1-25, and Col 5:50).

26. As per claims 57 and 64:

Djakovic teaches "The method of claim 55, where step (1) is performed using the Transmission Control Protocol, and wherein step (5) is performed using the User Datagram Protocol" in (Col 6 lines 50).

27. As per claims 58 and 65:

The method of claim 55, wherein step (6) is performed using an encryption key previously shared using a reliable communication protocol" in (Col 7:20-30).

28. As per claims 59 and 66:

Djakovic teaches "The method of claim 58, wherein the reliable communication protocol is the Transmission Control Protocol" in (Col 6 lines 50).

29. As per claim 61:

Djakovic teaches "A method of securely transmitting a plurality of data records to a remote computer using an unreliable communication protocol, comprising:

(1) "establishing a reliable connection with the remote computer" in (Col 7:20-30);

(2) "exchanging encryption credentials with the remote computer over the reliable connection" in (Col 7:20-30);

(3) "receiving a plurality of data records from the computer using an unreliable communication protocol such that each data record has been encrypted by generating a nonce (*a nonce is a random number. Djakovic teaches that random number generator is a true random sequence generators (Col 5 lines 35-44), which have the property that the generator's equences cannot be reproduced, even with the same input.)*" in (Col 4:1-25, and Col 5:50),

"encrypting text,

using the nonce to generate a message authentication code corresponding to the encrypted text, and appending the encrypted text, the nonce(*a nonce is a random number. Djakovic teaches that random number generator is a true random sequence generators (Col 5 lines 35-44), which have the property that the generator's equences cannot be reproduced, even with the same input)*, and the message authentication code to the data record" in (Col 4:1-25, and Col 5:50); and

(4) decrypting the encrypted text in each of the plurality of encrypted data records using the corresponding nonce extracted from each data record and a previously shared encryption key" in (Col 4:25-55).

However, Djakovic does not teach of "using the nonce to generate a message authentication code corresponding to the encrypted text".

Nevertheless, Bellare discloses the Block Cipher Mode of Operation For Secure, Length-Preserving Encryption" invention, which includes a method of generating a CBC message authentication code (MAC), and concatenate the CBC-MAC with ciphered block (Col 5 lines 5-20, Col 6 lines 50-56).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Djakovi's invention to incorporate Bellare's CBC-MAC teaching to further authenticate each cipher block.

30. As per claim 62:

The method of claim 61, further comprising checking to determine whether each data record received from the client computer is formatted according to a secure unreliable transmission format and, if a particular record is not formatted according to a secure unreliable transmission format, by passing the decryption using the corresponding nonce.

Response to Arguments

31. Applicant has amended claims 1, 6, 7, 10, 16, 21, 23, 25, 27, 29-30, 35, 38, 43, and newly added claims 49-67, which necessitated new grounds of rejection. See Rejections above.

Conclusion

32. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

33. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son
Examiner
Art Unit 2135

HOSUK SONG
PRIMARY EXAMINER